The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ARMANDO MONTALVO

Appeal 2007-1130
Application 09/688,609
Technology Center 2100

Decided: May 3, 2007

Before: JEAN R. HOMERE, JAY P. LUCAS, and MARC S. HOFF, *Administrative Patent Judges*.

HOFF, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF CASE

Appellant appeals under 35 U.S.C. § 134 (2002) from a final rejection of claims 1-10. We have jurisdiction under 35 U.S.C. § 6(b) (2002).

Appellant's invention relates to a system and method for secure communications. In the words of the Appellant:

Claim 1 recites a virtual biological fluid system 10 for secured communications and claim 10 recites a method for secure communications over a network. The system 10 of claim 1 includes a primary gateway that has security information. The system 10 also includes multiple communication layers 22 and a security control plane 20 that is coupled to and is formed using information from each of the communications layers 22. The security control panel 20 in conjunction with the security information forms a virtual biological fluid 40 that insures secure data transmission. The method of claim 10 has similar limitations as that of the system of claim 1 except security data is generated and utilized to form the virtual biological fluid. The method also includes the formation of a virtual biological fluid where communication between a ground gateway and a station 14 may occur. See page 4, line 9 through page 6, line 10 of the specification.

Claim 1 is exemplary:

1. A virtual biological fluid system for secure communications, said system comprising:

a primary gateway having security information;

a plurality of communication layers, and

a security control plane coupled to and formed using information from each of said plurality of communications layers, whereby said security control plane in conjunction with said security information forms a virtual biological fluid insuring secure data transmission.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Preston	US 2002/0032853 A1	Mar. 14, 2002
Willis	US 6,385,647 B1	May 7, 2002
Greene	US 6,578,145 B1	Jun. 10, 2003

The rejections as presented by the Examiner are as follows:

Group I: The Examiner rejected claims 1 and 10 under 35 U.S.C. § 103(a) as being obvious over Preston in view of Willis.

Group II: The Examiner rejected claims 2-9 under 35 U.S.C. 103(a) as being obvious over Preston in view of Willis and Greene.

Appellant contends that the claimed subject matter would not have been obvious, in that neither Preston nor Willis teaches a security control plane coupled to and formed using information from each of a plurality of communication layers. The Examiner contends that Preston does teach such a security apparatus, coupled to and using information from each of the communication layers.

Rather than repeat the arguments of Appellant or the Examiner, we make reference to the Briefs and the Answer for their respective details. Only those arguments actually made by Appellant have been considered in this decision. Arguments that Appellant could have made but chose not to make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2004).[1]

We affirm-in-part.

ISSUES

There are two principal issues in the appeal before us.

[1] Appellant have not presented any substantive arguments directed separately to the patentability of the dependent claims or related claims in each group, except as will be noted in this opinion. In the absence of a separate argument with respect to those claims, they stand or fall with the representative independent claim. *See In re Young,* 927 F.2d 588, 590, 18 USPQ2d 1089, 1091 (Fed. Cir. 1991). *See also* 37 C.F.R. § 41.37(c)(1)(vii).

The first issue is whether Appellant has shown that the Examiner failed to establish a prima facie case of obviousness, because no reference of record teaches a system insuring secure data transmission formed from a security control plane (itself formed using information from each of a plurality of communications layers) in conjunction with security information, as required by claims 1 and 3-10.

The second issue is whether Appellant has shown that the Examiner failed to establish a prima facie case of obviousness, because no reference of record teaches a satellite in orbit, the security control plane being present on board the satellite, as required by dependent claim 2.

FINDINGS OF FACT

Appellant invented a 'virtual biological fluid' system for secure communications, including in pertinent part "a security control plane coupled to and formed using information from each of said plurality of communications [sic] layers, whereby said security control plane in conjunction with said security information forms a virtual biological fluid insuring secure data transmission" (Cl. 1, ll. 5-8; Specification 5: 17-20 and 23-25). Appellant concedes that "phrases such as 'biological fluid' and 'cells'" merely highlight a conceptual analogy (Specification 4: 17-18), and that "the 'biological fluid' of the present invention is not really a fluid in the conventional sense but is a conceptual 'virtual' fluid" (Specification 4: 18-20). Because the words correspond to a mere concept or analogy, we accord the phrase "virtual biological fluid" no patentable weight,[2] and interpret the claims as being drawn to a system (or method) for secure communications.

Preston teaches a system for secure communications. Preston teaches a gateway having security information (Fig. 1: the entirety of secure dynamic link allocation system 110 corresponds to a "gateway" between computer systems ("nodes") 120 and 130; Para. [0035], [0040]-[0044]). Preston further teaches a plurality of communication layers (Fig. 1, application layer 142, presentation layer, session layer 152, transport layer 162, network layer 164, data link layer 166, and corresponding layers in receiving node 130; see also Figure 4, OSI layers 410). Preston further teaches a security manager (Fig. 1, element 158, 178; Para. [0038]) containing a content labeling and security authorization module 220 (Para. [0042]) which creates a content label 226 to be prepended to a message before encryption by an encryption module 228 (Para. [0044]). The "security manager" of Preston corresponds to the claimed security control plane.

Within sending node 120 of Preston, at least the application layer, presentation layer, and session layer are coupled to and send information to the security manager 158 (see Fig. 1). Within receiving node 130 of Preston, at least the physical layer (which corresponds to a wire or cable in a wire network: Para. [0058]), data link layer, network layer, and transport

[2] We also note that the Examiner had previously made a rejection of claims 1-10 under 35 U.S.C. 112, first paragraph, asserting that the phrase "virtual biological fluid" was not described in such a way as to enable one skilled in the art to make and/or use the invention. The decision to withdraw that rejection may merit further consideration.

layer are coupled to and send information to the security manager 178 (see Fig. 1).

Willis teaches a system for routing data via an IP network or via satellite, including a gateway having security information (Specification, col. 15, ll. 34-67; col. 16, ll. 1-56; Fig. 9, content provider gateway 1310).

Greene is directed to secure communication of personal identification numbers (PINs) between a security module and a plurality of secure keypad devices. Greene discloses relaying data from one (master) secure keypad 10 to one or more other ("satellite") secure keypads 11 (col. 8, ll. 47-54)

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of establishing a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). See also *In re Piasecki*, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The Examiner can satisfy this burden by showing that some objective teaching in the prior art or knowledge generally available to one of ordinary skill in the art suggests the claimed subject matter. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Only if this initial burden is met does the burden of coming forward with evidence or argument shift to the Appellant. *Oetiker*, 977 F.2d at 1445, 24 USPQ2d at 1444. See also *Piasecki*, 745 F.2d at 1472, 223 USPQ at 788. Thus, the Examiner must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the Examiner's conclusion.

References within the statutory terms of 35 U.S.C. § 102 qualify as prior art for an obviousness determination only when analogous to the claimed invention. *In re Clay*, 966 F.2d 656, 658, 23 USPQ2d 1058, 1060 (Fed. Cir. 1992). Two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved. *In re Deminski*, 796 F.2d 436, 442, 230 USPQ 313, 315 (Fed. Cir. 1986); see also *In re Wood*, 599 F.2d 1032, 1036, 202 USPQ 171, 174 (CCPA 1979) and *In re Bigio*, 381 F.3d 1320, 1325, 72 USPQ2d 1209, 1212 (Fed. Cir. 2004).

ANALYSIS

The Examiner correctly identifies the security manager 158 of Preston as corresponding to the claimed "security control plane" (Answer 8: 6-10). The security manager is "formed" using information from each of a plurality of communication layers (Fig. 1; Para. [0041]). The receiving node 130 of Preston contains an analogous security manager 178, which works as part of receiving system software 174 to reassemble, verify security, and decode messages as needed (Para. [0037]).

Because we find that each of the seven communication layers of Preston are coupled to and provide information to security managers 158 or 178, we are not persuaded by Appellant's argument that "neither Preston nor Willis ... teaches or suggests the limitations of a security control plane coupled to and formed using information from each of multiple communication layers" (Br. 10: 12-14), or that "Preston only discloses the use of information from a single communication layer" (Br. 11: 21-22).

We are not persuaded by Appellant's argument that Preston fails to meet the limitations of claim 1 because "security information is not passed from the communication layers ... of Preston to the security managers 158 and 178 rather communication messages are passed" (Br. 11: 1-2). The claims merely recite that "information" is used to "form" the security control plane. Communication messages constitute "information" just as surely as "security information" does.

Appellant argues that Preston does not teach the formation of a "virtual biological fluid," which "enables the use of an interactive security doctrine that allows for multiple levels of security deployment" (Br. 14: 5-7). We note that the claims do not recite such an "interactive security doctrine" or "multiple levels of security deployment." As mentioned *supra*, we further note that Appellant describes the "biological fluid" as a mere "conceptual 'virtual' fluid" (Specification 4: 18-20); that the fluid "can be used to develop intrusion detection techniques" (Specification 5: 25-26), but that Appellant does not explain how this may be done; that the fluid "enables the present invention to use an interactive security doctrine that allows for multiple levels of security deployment" (Specification 5: 26 to Specification 6: 1), but that Appellant does not explain how this may be done. Because of the absence of any explanation in Appellant's disclosure, we decline to read into Appellant's claim recitations of "virtual biological fluid," the unclaimed characteristics Appellant urges in the Brief.

Appellant argues that the Willis reference is nonanalogous art, in that "Willis is directed to the efficiency of data communication not the security thereof" (Br. 15: 11-12) and "[t]he system of Willis would not have logically commended itself to the Applicant's attention in solving the problems associated with secure communication" (Br. 15: 14-16). Appellant claims a system and method "insuring secure data transmission" (Cl. 1: 7-8), and admits that Willis uses a secure data transfer protocol (Br. 15: 12-13). We conclude that Willis's invention, being directed to transmitting data efficiently and securely, is reasonably pertinent to the particular problem (i.e., secure data transmission) with which the inventor is involved.

Because we find that Preston teaches elements that read on the claimed "gateway," we agree with the Examiner that it would have been obvious as well to include a gateway as taught by Willis, having security information, because Willis teaches that its gateway "reduce[s] the risk of exposing [sensitive] information to interception by third parties (Willis, col. 15, ll. 34-45).

With regard to claim 3,[3] Preston clearly shows an application layer coupled to security manager 158 via virtual sockets 154, providing information thereto (Figs. 1, 2A). With regard to claim 4, Preston (Fig. 1)

[3] In the application as filed, claims 3-9 each depended from claim 2. In Appellant's amendment filed July 19, 2004, claims 3-9 were identified as "Original," but each claim now depended from claim 1. During subsequent prosecution, the claims remained dependent from claim 1, and neither the Examiner nor the Appellant raised the issue. Because the Examiner stated in the Examiner's Answer that "the status of claims contained in the brief is correct," we treat claims 3-9 as written in the Claims Appendix, each dependent from claim 1.

associates a presentation layer with application layer 142. Preston further teaches that control in a communication network is passed from the application layer to the presentation layer (Para. [0058]; Fig. 4, application layer 7, presentation layer 6).

With regard to claim 5, Appellant concedes that Preston discloses the use of information by security manager 158 from session layer 152 (Br. 11: 21-22).

With regard to claims 6-9, Preston teaches a transport layer, network layer, data link layer, and physical layer (Fig. 1, all within receiving system software 174) coupled to and providing information to security manager 178.

The Examiner relies on Greene to teach "said security control plane [being] on board [a] satellite" in orbit, as recited in claim 2. As noted above, however, Greene discloses relaying data from one (master) secure keypad 10 to one or more other ("satellite") secure keypads 11 (col. 8, ll. 47-54). Greene does not disclose any data communication security hardware or software located on board a satellite in orbit. Because the Examiner does not provide a reference teaching a security control plane on board a satellite in orbit,[4] we cannot sustain the Examiner's rejection of claim 2.

[4] That we find the teachings of Greene insufficient to meet the claim does not mean we are certain that no pertinent prior art exists.

CONCLUSION OF LAW

Based on the findings of fact and analysis above, we conclude that the Examiner did not err in rejecting claims 1 and 3-10. The rejection of those claims is affirmed.

We conclude that the Examiner erred in rejecting claim 2. The rejection of claim 2 is reversed.

DECISION

The Examiner's rejection of claims 1 and 3-10 is affirmed. The Examiner's rejection of claim 2 is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED-IN-PART

tdl

Hughes Electronics Corporation
Corporate Patents & Licensing
Bldg. R11, Mall Station
P.O. Box 956
El Segundo, CA 90245-0956